(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 645 688 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 94202652.7

(51) Int. Cl.[6]: G06F 1/00

(22) Date of filing: 16.09.94

(30) Priority: 21.09.93 NL 9301633

(43) Date of publication of application:
29.03.95 Bulletin 95/13

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU NL PT SE

(71) Applicant: Koninklijke PTT Nederland N.V.
P.O. Box 95321
NL-2509 CH The Hague (NL)

(72) Inventor: van den Bos, Marius Jan Bartele
Riesven 23
NL-9302 EL Roden (NL)
Inventor: Steenbeke, Johannes Gerhardus Marinus
Otto Eerelmanstraat 14
NL-9718 JZ Groningen (NL)
Inventor: de Jager, Paul
Geerakkers 11
NL-9468 EV Annen (NL)
Inventor: Stinesen, Vincentius Wilhelmus
Poelestraat 23E
NL-9711 PH Groningen (NL)

(54) Method for the identification of users of telematics servers.

(57) Telematics system, comprising a telecommunications system and an independent identification server, suitable and designed for identification and possibly verification of subscribers who wish to make use of telematics servers likewise linked to said telecommunications system. The identification server works for a plurality of telematics servers, as a result of which the identification/verification procedure is uniform for all those telematics servers.

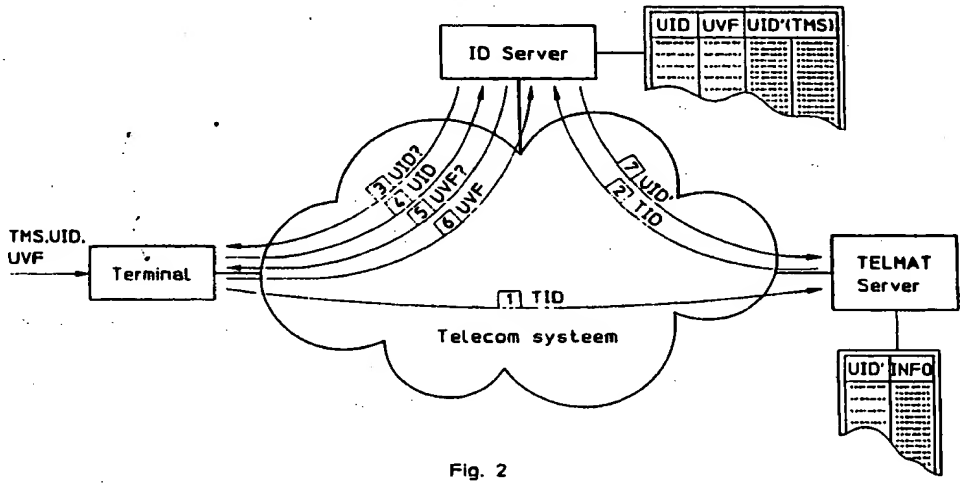

Fig. 2

EP 0 645 688 A1

terminal and the identification server, and the terminal or a terminal server transmitting a terminal identifier (TID) to the identification server, the user further sending his user identifier (UID) to the identification server, which compares this with user identifiers previously stored in the identification server and, in the event of agreement between one of said stored user identifiers and the identifier received, sends said identifier or an image thereof (UID') to a telematics server selected by the user. The invention also comprises an identification server which is eminently able to form part of the telematics system according to the invention.

C. REFERENCES

None.

D. ILLUSTRATIVE EMBODIMENTS

Fig. 1 shows, in the form of a diagram, a first illustrative embodiment of a telematics system according to the invention in which the method presented can be implemented. Fig. 2 shows a slightly different illustrative embodiment.

Fig. 1 shows a telecommunications system to which a terminal is connected, an identification server and a telematics server, for example a computer system for on-line enquiry for data. Via the terminal - for example a PC with modem and communications software - a user can activate a telecommunications link to the telematics server required. At the same time - or directly afterwards - a link can be activated to the identification server. Via the first link, a terminal identifier TID is sent to the selected telematics server (1); via the last link, the same terminal identifier TID is sent to the identification server, together with a code TMS which indicates the telematics server selected (2). Said identification server then carries out an identification protocol which consists in the identification server asking the user for his user identifier VID (3), the user sending the latter (4), and the latter being looked up by the identification server in a register containing user identifiers. At the same time, an associated user verifier is looked up, as well as user codes UID' applicable to the different telematics servers (one user can be known under different user codes to different telematics servers). The user is then asked for his verifier (password) (5), the user sends the latter (6), and that verifier is compared with the verifier from the register. In the event of agreement, a link is activated, on the basis of the telematics server TMS selected, to that telematics server, and the terminal identifier TID and the user code (from the register of the identification server) is sent to the telematics server (7). A better method of verification is, for example, the "challenge signed response" method. This involves the user sending his verifier to the identification server, after which the identification server sends a random code string to the user who enciphers this string with a secret key (for example stored in a smart card) and sends the encipherment result to the identification server. The identification server deciphers that enciphered string with the aid of a key which is related to the verifier received. Thus the user can prove his identity. Then, links between the terminal and the identification server, and between the identification server and the telematics server are broken, and the user is able to exchange messages via the link between his terminal and the telematics server selected, no further identification/verification procedure being necessary. After receiving the user code UID', the telematics server has also been able to find previously stored further user data, for example concerning the settling of charges relating to the use of the service.

The illustrative embodiment shown diagrammatically in Fig. 2 differs from the above illustrative embodiment insofar as the telematics server, after receiving the terminal identifier TID from the terminal (1), activates a link to the identification server and via this link sends the terminal identifier (2). Thereupon, the identification server activates a link to the terminal and asks for the user identifier UID of the user (3). The verification protocol proceeds as indicated above (4, 5, 6). In the event of a positive result, the user code UID', valid for the telematics server selected, of the user is sent to the telematics server which then breaks the link to the identification server. The link between the identification server and the terminal is also broken, and further messages are exchanged between the terminal and the telematics server. In the case of this last option, the TID is therefore not sent directly to the identification server, as for the first option, but via the telematics server. After the TID has been received, the identification server activates a link to the terminal whose TID had been received.

The identification server thus serves for executing an identification and verification protocol (log-in protocol) for any other telematics server. The advantage is that users always deal with the same identification server and are always able to log in in the same manner and always using the same identifier and verifier, even if the telematics servers change. This method is eminently applicable in an ISDN system in which one terminal is able to activate two links simultaneously, in this case to the identification server and the telematics server. ISDN is not a precondition, however, since the links need not necessarily be active simultaneously, but may alternatively be activated successively.

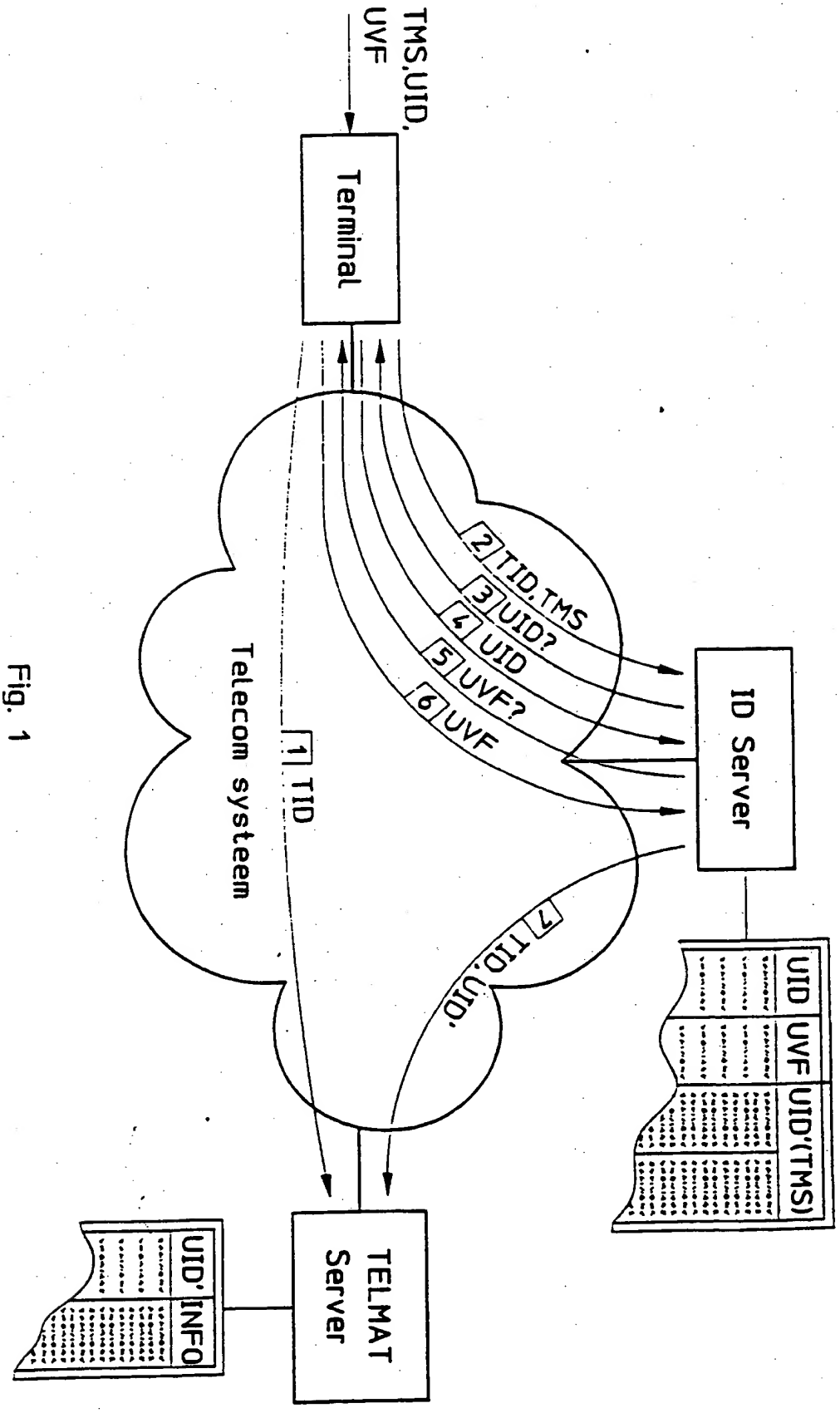

Fig. 1

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 94 20 2652

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP-A-0 456 386 (ICL) * figures 1,2 * * page 3, line 39 - page 5, line 43 *	1,2,4-8	G06F1/00
A	US-A-5 113 499 (ANKNEY ET AL.,) * figures 1,2A,2B,6,7,9 * * column 8, line 25 - column 10, line 68 *	1-3,5-8	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	2 December 1994	Weiss, P

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)